REMARKS

Claim Status

Claims 1-13 are now pending, with claims 1, 11 and 12 being in independent form. Claims 1-6, 8, 9 and 11-13 have been amended. The amendments to claims 2, 3, 5, 6, 8, 9 and 13 are merely cosmetic or clarifying in nature. Support for the amendments to independent claims 1, 11 and 12 may be found, for example, at pg. 5, lines 1-13 of the specification as originally filed. Additional support for the amendment to claim 4 may be found, for example, in FIG. 1 and at pg. 5, lines 26-27 of the specification as originally filed. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

Claim 4 has been objected to based on a minor informality. Withdrawal of this objection is in order, as explained below.

Claims 1 and 12 stand rejected under 35 U.S.C. §112, second paragraph, as indefinite for failure to particularly point out and claim the subject matter which applicants regard as the invention. Withdrawal of this rejection is also in order, as explained below.

Claim 11 stands rejected under 35 U.S.C. §101 as directed to non-statutory subject matter. Withdrawal of this rejection is also in order, as also explained below.

Claims 1-13 stand rejected under 35 U.S.C. §102(a) as anticipated by "Clustering Intrusion Detection Alarms to Support Root Cause Analysis", IBM Research, Zurich Research Laboratory, ACM Transactions on Information System Security, Vol. 6, No. 4, pgs. 443-474, November 2003 ("*Julisch*").

Applicants have carefully considered the Examiner's rejections, and the comments provided in support thereof. For the following reasons, applicants respectfully assert that all claims now pending in the present application are patentable over the cited art.

Amendments Addressing Section 112 Issues and Formalities

The Examiner has stated that "'the limitation supplying alert identifiers satisfying the request and whose description cannot be refined with respect to said request' has [been] repeated twice in this claim". Applicants have amended claim 4 in a self-explanatory manner. Withdrawal of this objection is deemed to be in order.

The Examiner stated that "the limitations 'values attributes' in line 6 and 'a plurality of attribute domains' in line 8-9" of claims 1 and 12 lack sufficient antecedent basis. In response to these rejections, applicants have amended the claims to address each such rejection in a self-explanatory manner. Accordingly, withdrawal of these rejections is also deemed appropriate.

Descriptive Summary of the Prior Art

Julisch discloses an alarm-clustering method that supports a human analyst in identifying root causes of intrusion system triggers to permit identification and removal of the most predominant and persistent root causes.

Summary of the Subject Matter Disclosed in the Specification

The following descriptive details are based on the specification. They are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations which are unclaimed.

The specification discloses a method of managing alerts issued by intrusion detection sensors of an information security system including an alert management system, where each alert is defined by an alert identifier and alert content. The disclosed method comprises associating, with each of the alerts issued by the intrusion detection sensors, a description that includes a conjunction of valued attributes belonging to attribute domains. The valued attributes

belonging to each attribute domain are organized into a taxonomic structure defining generalization relationships between said valued attributes, where a plurality of attribute domains forms a plurality of taxonomic structures.

The description of each of the alerts is completed with sets of values that are induced by the taxonomic structures based on the valued attributes of the alerts to form complete alerts. These complete alerts are stored in a logic file system to enable the complete alerts to be consulted. Here, each complete alert is saved in the logic file system as a file with the completed description of each complete alert expressed using propositional logic.

The disclosed method thus provides a simple method of managing alerts issued by intrusion detection sensors to enable flexible, easy and rapid consultation of such alerts.

Patentability of Independent Claim 11 under 35 U.S.C. §101

The Examiner (at pg. 3-4 of the Office Action) has stated that:

> Claim 11 is interpreted as being purely software per se because it comprises merely software for manipulating data.... Data structure not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer.... In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory.

In response to the foregoing, applicants have amended claim 11 to place it into independent form, such that claim 11 now recites a computer readable medium encoded with a computer program executed by a computer that causes an alert management system to manage alerts issued by intrusion detection sensors. Independent claim 11 now also recites that the computer program includes the program code for executing each corresponding method step of independent claim 1. In view of the foregoing, independent claim 11 as now amended is directed

to statutory subject matter, reconsideration and withdrawal of the rejection under 35 U.S.C. §101 are accordingly deemed to be in order, and notice to that effect is requested.

Patentability of the Independent Claims Under 35 U.S.C. §102(a)

Independent claim 1 has been amended to recite, *inter alia*, "wherein each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic". Independent claims 11 and 12 have been correspondingly amended. Support for this amendment to independent claims 1, 11 and 12 may be found, for example, at pg. 5, lines 1-13 of the specification as originally filed.

The Examiner (at pg. 4 of the Office Action) asserts that:

> Julisch discloses ... storing said complete alerts in a logic file system (21) to enable them to be consulted (Julisch: page 450, section 4 [ALARM-CLUSTERING PROBLEMS] and pages 456-457, section 5.1 and 463-465, "alarm log").

Applicants disagree that *Julisch* teaches or suggests the express recitations of now amended independent claims 1, 11 and 12.

Julisch (pg. 450; FIG. 1(b)) teaches that the variable a is used to identify a first alarm in the alarm log depicted in FIG. 1(b). The alarm logs disclosed in *Julisch* are not generalized alarms but, rather, alarms that have been detected, i.e., alarms that are provided to a heuristic algorithm that is used to provide a solution to the disclosed alarm-clustering problem. The *generalization* discussed in *Julisch* is, in fact, with respect to IP addresses and port numbers, not the alarm itself.

Applicants' claimed invention differs in an important manner from the teachings of *Julisch*. The processed alarms (i.e., the claimed "complete alerts") are stored in a logic file system. *Julisch* (pg. 457; FIG. 2), on the other hand, teaches a relational database (T) that is used to store a set of detected alarms. In particular, *Julisch* describes that the set of detected

alarms, which have been respectively stored into the alarm log upon detection, are copied into the relational database (T) for further processing. However, this relational database (T) is not equivalent to the logic file system of independent claims 1, 11 and 12 that stores complete alerts (see pg. 457; FIG. 2). Indeed, *Julisch* fails to teach or suggest anything whatsoever with respect to the use of such a logic file system.

As described at pg. 5, lines 1-3, the claimed logic system may comprise an LISFS, which is disclosed in a paper by Padioleau and Ridoux entitled "A Logic File System" that was presented at the Usenix Annual Technical Conference in 2003. Independent claims 1 and 12 each specify how complete alerts are stored, i.e., each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic. Independent claim 11 correspondingly recites this feature. *Julisch* fails to teach or suggest this express and important limitation.

Storing complete alerts in a logic file system advantageously enables a security operator to consult an alert management system in an efficient, quick and flexible manner to obtain a precise view of all alerts issued by intrusion detection sensors (see pg. 2, lines 33-37 of the instant specification). Moreover, the complete description is expressed using propositional logic. As a result, it becomes possible to more efficiently and advantageously consult complete alerts and/or successively browse the alerts in the set of complete alerts. *Julisch* fails to teach or suggest applicants' claimed invention that encompasses such advantageous features and functionality.

In view of the foregoing, amended independent claims 1, 11 and 12 are not anticipated by *Julisch*. Reconsideration and withdrawal of the rejection of claims 1, 11 and 12 under 35 U.S.C. §102 are thus deemed to be in order, and early notice to that effect is solicited.

Moreover, by virtue of the above-discussed differences between the recitations of claims 1, 11 and 12 and the teachings of *Julisch*, and the lack of any clear motivation for modifying

Julisch to achieve applicants' claimed invention, independent claims 1, 11 and 12 are likewise deemed to be patentable over *Julisch* under 35 U.S.C. §103.

Dependent Claims

In view of the patentability of independent claims 1, 11 and 12 for the reasons presented above, each of dependent claims 2-10 and 13 is respectfully deemed to be patentable therewith over the prior art. Moreover, each of these claims includes features which serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are once more solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: October 7, 2008